

# Improved wavelength attack on practical continuous variables quantum key distribution system with heterodyne protocol

Xiang-Chun Ma, Shi-Hai Sun, Mu-Sheng Jiang and Lin-Mei Liang\*

*Department of Physics, National University of Defense Technology, Changsha 410073, P.R.China*

We present the wavelength attack on practical continuous variables quantum key distribution system with heterodyne protocol, in which the transmittance of beam splitters at Bob's station is wavelength-dependent. Our strategy is proposed independently analogous to that of Han's group (arxiv: 1206.6550v1), but in Han's paper the shot noise of the two beams that Eve sends to Bob transmitting after the homodyne detectors is unconsidered. However, shot noise is the main contribution to the deviation of Bob's measurements from Eve's when implementing the wavelength attack, so it must be considered accurately. In this paper, we firstly analyze the solutions of the equations specifically that must be satisfied in this attack, which is unconsidered rigorously in Han's paper. Then we calculate the shot noise of the homodyne detectors accurately and conclude that the wavelength attack can be implemented successfully in some parameter regime.

PACS numbers: 03.67.Hk, 03.67.Dd, 89.70.Cf

## I. INTRODUCTION

Continuous variables quantum key distribution (CVQKD), which is an alternative of single photon quantum key distribution (QKD), has many advantages, such as high repetition rate of communication, high detection efficiency and ease of integration with standard telecom components, so it has been paid much more attention in recent years [1–7]. However, in practical system because there exist some imperfections such as loss or noise, the unconditional security of final key of QKD may be compromised. It is extensively investigated in single photon QKD, like PNS attack etc. [8–12], but not more in CVQKD [13, 14]. This is because the system of CVQKD is one way communication system and needs less optical elements than two ways. Furthermore, most of intervention of Eve on the system of CVQKD can be detected by the parameter estimation of classical post-processing of CVQKD.

In Ref. [15], the wavelength-dependent property of beam splitter (BS) was explored by eavesdropper Eve to attack single photon QKD successfully. Subsequently, Han's group extended this attack, so called wavelength attack, to the all-fiber system of CVQKD [16]. However, in Han's paper, there exist two significant problems not being considered. First, the equation that must be satisfied in this attack, so called *attacking equation*, was not solved specifically in some permitted parameter regime, which may make this attack invalid. Second, the shot noise of the two beams that Eve sends to Bob, when transmitting through the homodyne detectors, was neglected too. However, shot noise is the main contribution to the deviation of Bob's measurements from Eve's when implementing the wavelength attack, so it must be considered accurately.

In this paper, we demonstrate and resolve the two

problems of Han's paper, and then we improve the wavelength attack method against all-fiber CVQKD system by tuning the attacking parameter's regime. Finally, we conclude that the wavelength attack will be implemented successfully in some parameter regime. The following is organized as: In Sec. II, we demonstrate the wavelength attack and solve the attacking equations specifically. Then, we analyze the shot noise introduced by the one-port and two-port homodyne detectors and calculate the conditional variance between the two legitimate parties Alice and Bob considering the deviations introduced by the shot noise. Finally, in Sec. III, we make some discussions and conclusions about the feasibility of this wavelength attack on practical CVQKD system based on the conditional variance obtained in Sec. II B.

## II. WAVELENGTH ATTACK ON PRACTICAL CVQKD SYSTEM

### A. Scheme of wavelength attack

In practical CVQKD system, Alice first modulates a coherent state ( $\hat{x}_A, \hat{p}_A$ ) by amplitude and phase modulators according to bivariate Gaussian distributions centered on  $(x_A, p_A)$  of variance  $V_A N_0$ , where  $N_0$  is the shot noise variance that appears in the Heisenberg relation  $\Delta x \Delta p \geq N_0$  [3],

$$\begin{aligned}\hat{x}_A &= x_A + \hat{x}_N^A, \\ \hat{p}_A &= p_A + \hat{p}_N^A.\end{aligned}\tag{1}$$

And  $\langle (\hat{x}_N^A)^2 \rangle = N_0$ ,  $\langle (\hat{p}_N^A)^2 \rangle = N_0$ , then, she sends this state to Bob through a quantum channel optical fiber and Bob implements a homodyne or heterodyne detection after receiving this state. So, after many repetitions, Alice and Bob can share trains of correlated data and then get the final key after the classical data post-processing procedure. However, because the practical system may

---

\* nmliang@nudt.edu.cn

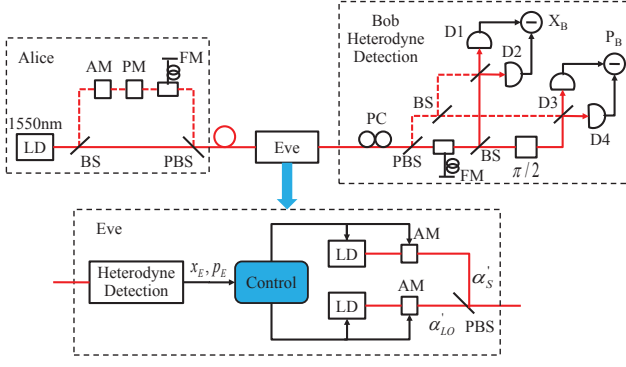


FIG. 1. (Color online) Wavelength attack setup on practical CVQKD system with heterodyne detection (dashed red line indicates signal beam and solid red line local oscillator)[16]. LD: laser diode; AM: amplitude modulator; PM: phase modulator; FM: Faraday mirror; BS: beam splitter; PBS: polarization beam splitter; PC: polarization controller; D: photodetector.

have some imperfections which will leave the loophole to the potential eavesdropper Eve, we must timely calibrate the system carefully and make efforts to eliminate all the existing loopholes.

Generally, the transmittance of some practical beam splitters depends on the wavelength of beams, namely  $T = F^2 \sin^2(\frac{c\omega\lambda^{2.5}}{F}) \equiv T(\lambda)$ , where  $F^2$  is the maximal power that is coupled,  $c$  is the coupling coefficient,  $\omega$  is the heat source width[17, 18]. Consequently, as Ref. [16] proposed, Eve can use this wavelength dependent property to attack the practical CVQKD system with heterodyne protocol shown in Fig. 1. She can send two beams whose wavelength and intensity can be tuned to control Bob's measurement results, which are made identical to Eve's.

Specifically speaking, Eve first intercepts Alice's sending states and makes a heterodyne detection on them, so she can get the quadratures  $x_E, p_E$ , which can be given by

$$\begin{aligned}\hat{x}_E &= \hat{x}_A + \hat{x}_N^E, \\ \hat{p}_E &= \hat{p}_A + \hat{p}_N^E,\end{aligned}\quad (2)$$

where  $\langle (\hat{x}_N^E)^2 \rangle = N_0$ ,  $\langle (\hat{p}_N^E)^2 \rangle = N_0$  is the shot noise introduced by Eve's heterodyne detection. Then, she sends to Bob two beams whose intensities are denoted as  $|\alpha'_S|^2$  and  $|\alpha'_{LO}|^2$  respectively. Because the interference between these two beams are destroyed, Eve might be able to control the intensities and wavelength of them to make these two beams, after transmitting Bob's heterodyne detectors, satisfy

$$\begin{aligned}(1-T_1)(1-2T_1)|\alpha'_S|^2 - (1-T_2)(1-2T_2)|\alpha'_{LO}|^2 &= \sqrt{\eta}x_E|\alpha_{LO}|, \\ T_1(1-2T_1)|\alpha'_S|^2 - T_2(1-2T_2)|\alpha'_{LO}|^2 &= \sqrt{\eta}p_E|\alpha_{LO}|,\end{aligned}\quad (3)$$

where  $T_1(T_2)$  represents the transmittance of practical beam splitter corresponding to the beam  $\alpha'_S(\alpha'_{LO})$  whose

wavelength is  $\lambda_1(\lambda_2)$ .  $\alpha_{LO}$  is the amplitude of local oscillator in absence of this wavelength attack,  $\eta$  is the channel loss. After scaling with  $\sqrt{2}\alpha_{LO}$ [16], then, Bob will get measures  $\sqrt{\eta}x_E/\sqrt{2}$  and  $\sqrt{\eta}p_E/\sqrt{2}$ . Thus, the wavelength attack may succeed, however, whether Eqs. (3) have the real solutions or not in practical parameter regime determines the validity of this wavelength attack. So, in what follows we'll analytically investigate the solutions of Eqs. (3) in permitted parameter regime.

First, we rewrite Eqs. (3) as

$$\begin{aligned}(1-T_1)(1-2T_1)|\alpha'_S|^2 &= \sqrt{\eta}x_E|\alpha_{LO}| + (1-T_2)(1-2T_2)|\alpha'_{LO}|^2, \\ T_1(1-2T_1)|\alpha'_S|^2 &= \sqrt{\eta}p_E|\alpha_{LO}| + T_2(1-2T_2)|\alpha'_{LO}|^2.\end{aligned}\quad (4)$$

Provided  $\alpha'_{LO}$  is the same as  $\alpha_{LO}$ , then  $T_2$  is 1/2, Eqs. (4) will be reduced to

$$\begin{aligned}(1-T_1)(1-2T_1)|\alpha'_S|^2 &= \sqrt{\eta}x_E|\alpha_{LO}|, \\ T_1(1-2T_1)|\alpha'_S|^2 &= \sqrt{\eta}p_E|\alpha_{LO}|.\end{aligned}\quad (5)$$

As Ref. [16] says, generally,  $x_E, p_E$  are very small in practical implementation of CVQKD, Eqs. (5) are always solvable if  $x_E, p_E$  are both positive or negative at the same time. That's

$$\frac{1-T_1}{T_1} = \frac{x_E}{p_E}, \quad T_1 = \frac{p_E}{x_E + p_E} \in [0, 1]. \quad (6)$$

However, when  $x_E, p_E$  are different in sign,  $T_1 \notin [0, 1]$ . But by virtue of opting for an appropriate  $T_2 (\neq 1/2)$ , we are always able to confirm both of the right hand side of Eqs. (4) being either positive or negative at the same time, because both the second term on the right hand side of Eqs. (4) are the same in sign. Hence, Eqs. (4) or Eqs. (3) always hold if we select appropriate  $\alpha'_{LO}$ .

Additionally, we point out that we can always make the right hand side of Eqs. (4) enough small and  $T_2$  close to 1/2, thus  $|\alpha'_S|^2$  in the left hand of Eqs. (4) can always be small too, especially in discrete modulation protocol of CVQKD [4, 5] in which the signal intensity is always on single photon level. Consequently, this attack cannot be avoided efficiently even if Bob added a wavelength filter on his system before detectors, which is the same case in Ref. [15]. Because such extreme weak signal is still able to transmit through practical filter just by increasing the intensity of the incoming light and the wavelength of fake local oscillator can be close to the original one which is 1550nm. Laser after transmitting through the practical filter is permitted to have a line width, so the fake local oscillator cannot be filtered either.

Consequently, implementing this wavelength attack, theoretically, Eve can control her attacking parameters to make Bob's measurements identical with her or rather Eve completely knows Bob's measures. However, in Eqs. (3) we don't consider the interference between Eve's sending beams and vacuum mode entering from other port of beam splitters of Bob's apparatus as Fig. 1 shows, which could introduce excess noise into Bob's measurements, thus leading them deviate from Eve's. We will demonstrate it in next section.

### B. Deviation of Bob's measurements from Eve's and Alice's

As the previous section demonstrated, the interference with vacuum mode will lead Bob's measurements deviate from Eve's. And if the deviation is unfortunately large, Alice and Bob will find that they can't distill any secure keys because Bob's measures are too noisy from her after comparing partial data within parameter estimation phase of data post-processing. So, we must calculate the conditional variance between Alice and Bob to see whether Eve's wavelength attack could be successful or not. And we point out that the shot noise introduced by Bob's detectors is the main contribution of the conditional variance, which is not noted in Han's paper. We begin this calculation by analyzing the quantum noise of unbalanced homodyne detectors first and use the results to apply to Bob's apparatus.

#### 1. Quantum noise on unbalanced homodyne detectors

Homodyne detectors are extensively exploited to measure weak signal with bright local oscillator [19–21]. As depicted in Fig. 2, when the transmittance of beam splitter  $T=1/2$ , the homodyne detectors are balanced homodyne detectors (BHD), or else are unbalanced homodyne detectors (UBHD). Fig. 2(a) is two-port homodyne detectors with a subtractor, and Fig. 2(b) is one-port homodyne detectors without subtractor. Those two-port or one-port homodyne detectors can be used to measure weak signal's quadratures or vacuum state's quantum noise.

Generally, two-port balanced homodyne detectors can measure the quadratures  $x_A$  or  $p_A$  of weak signal  $\alpha_S$ , between which and the local oscillator the relative phase

is  $\theta$ . The measurement is

$$x_\theta = 2|\alpha_{LO}|(x_{in} \cos \theta + p_{in} \sin \theta), \quad (7)$$

and  $x_{in} = x_A + x_N, p_{in} = p_A + p_N$ .  $x_N, p_N$  are the vacuum noise, of which the variance is  $N_0$  [21]. The variance of  $x_{in}, p_{in}$  is

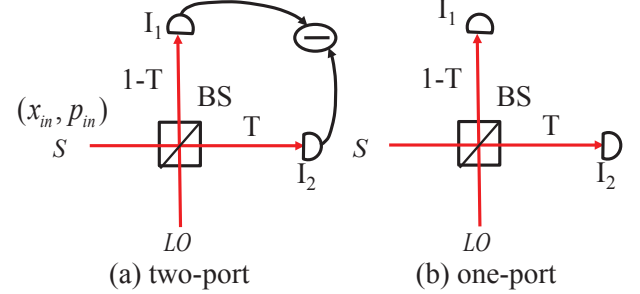


FIG. 2. (Color online) Unbalanced homodyne detectors with (a) two-port or (b) one-port.

$$\begin{aligned} \langle x_{in}^2 \rangle &= \langle x_A^2 \rangle + \langle x_N^2 \rangle = V_A + N_0, \\ \langle p_{in}^2 \rangle &= \langle p_A^2 \rangle + \langle p_N^2 \rangle = V_A + N_0, \end{aligned} \quad (8)$$

where  $V_A$  is the signal's variance. When  $V_A = 0$ , the output is the shot noise  $N_0$ . However, with unbalanced two-port homodyne detectors, the measurement will be different from the one in Eq. (7). The follows are the analysis of this case. Since the amplitude of signal and local oscillator can be designated by

$$\begin{aligned} \alpha_S &= |\alpha_S|e^{-i(\omega t + \phi)}, \\ \alpha_{LO} &= |\alpha_{LO}|e^{-i(\omega t + \theta)}, \end{aligned} \quad (9)$$

of which  $\phi$  and  $\theta$  are the modulated phase respectively, after transmitting the beam splitter, the intensity of local oscillator and signal can be written as

$$\begin{aligned} I_1 &= |\sqrt{1-T}\alpha_S + \sqrt{T}\alpha_{LO}|^2 = (1-T)|\alpha_S|^2 + T|\alpha_{LO}|^2 + \sqrt{T(1-T)}(\alpha_S^* \alpha_{LO} + \alpha_{LO}^* \alpha_S) \\ &= (1-T)|\alpha_S|^2 + T|\alpha_{LO}|^2 + \sqrt{T(1-T)} \times 2|\alpha_{LO}|(x_{in} \cos \theta + p_{in} \sin \theta), \\ I_2 &= |\sqrt{T}\alpha_S - \sqrt{1-T}\alpha_{LO}|^2 = T|\alpha_S|^2 + (1-T)|\alpha_{LO}|^2 - \sqrt{T(1-T)}(\alpha_S^* \alpha_{LO} + \alpha_{LO}^* \alpha_S) \\ &= T|\alpha_S|^2 + (1-T)|\alpha_{LO}|^2 - \sqrt{T(1-T)} \times 2|\alpha_{LO}|(x_{in} \cos \theta + p_{in} \sin \theta). \end{aligned} \quad (10)$$

Then, with the subtraction of  $I_1$  and  $I_2$ , the output can be obtained as

$$X_\theta = 2\sqrt{T(1-T)}x_\theta + (1-2T)(|\alpha_S|^2 - |\alpha_{LO}|^2), \quad (11)$$

where  $x_\theta$  has been given by Eq. (7) and when  $T = 1/2$  Eq. (11) is reduced to Eq. (7). If the weak signal is vacuum state, the amplitude of it can be read as  $\alpha_S = \langle \alpha_S \rangle + \delta\alpha_S$ , and  $\langle \alpha_S \rangle = 0$ , so  $x_A = p_A = 0$  and  $|\alpha_S|^2 = |\delta\alpha_S|^2 \equiv |\delta\alpha|^2 \ll |\alpha_{LO}|^2$ .  $\delta\alpha$  describes the amplitude

fluctuation of vacuum state. Neglect its square terms, then the output of UBHD is

$$X_\theta = 2\sqrt{T(1-T)}x'_\theta - (1-2T)|\alpha_{LO}|^2, \quad (12)$$

where  $x'_\theta$  is obtained from Eq. (7) by  $x_A = p_A = 0$ . When  $\theta$  is selected to be 0 or  $\pi/2$ , we can get the shot noise of the output  $4T(1-T)N_0$  denoted as  $(\Delta X)^2$  or  $(\Delta P)^2$  ( $(\Delta X)^2 = (\Delta P)^2 = 4T(1-T)N_0$ ), which is consistent with the one of BHD output when  $T = 1/2$ . The

right hand of Eq. (12) except the first term is the two ports' subtraction of the intensity of local oscillator because of the unbalanced splitting rate of the asymmetric beam splitter (ABS).

Subsequently, let's analyze the unbalanced one-port homodyne detectors. As shown in Fig. 2(b), the intensity of local oscillator and signal after transmitting the unbalanced beam splitter respectively has been already obtained by Eq. (10). When the weak signal is vacuum state, the intensity of Eq. (10) can be reduced to

$$\begin{aligned} I_1 &= T|\alpha_{LO}|^2 + \sqrt{T(1-T)}2|\alpha_{LO}|X_N, \\ I_2 &= (1-T)|\alpha_{LO}|^2 - \sqrt{T(1-T)}2|\alpha_{LO}|X_N, \end{aligned} \quad (13)$$

where  $X_N \in \{x_N, p_N\}$  and  $\theta$  has been selected to be 0 or  $\pi/2$ . The right hand side of Eqs. (13), except the first term which is unbalanced part of splitting of the bright local oscillator because of asymmetric splitting rate of ABS, is the fluctuation of each port of unbalanced one-port homodyne detectors respectively. With the two-port and one-port UBHD, we can compute the noise of the beams Eve sends to Bob in the next section. However, keep in mind that the noise of UBHD is introduced by the vacuum state from the other input port of asymmetric beam splitter of UBHD.

## 2. Conditional variance between Alice and Bob

Looking back to see Fig. 1 again, it's clear that there are two types of UBHD. On one hand, the first ABS at

Bob's station through which the signal or local oscillator transmits alone can be viewed as one-port UBHD, and each port output is the interference between vacuum state and either signal or local oscillator. So, as Sec. IIB1 analyzed, the intensity of first ABS output is (taking the signal beam as an example and the local oscillator is analogous),

$$\begin{aligned} I_S^r &= (1-T_1)I_S - 2\sqrt{T_1(1-T_1)}I_S X_N, \\ I_S^t &= T_1 I_S + 2\sqrt{T_1(1-T_1)}I_S X_N. \end{aligned} \quad (14)$$

And  $I_S$  is the intensity of the signal beam Eve sends, that's  $I_S = |\alpha'_S|^2$ . On the other hand, the second ABS is two-port UBHD, but the output is the interference between signal beam and vacuum state in addition to the one between local oscillator and vacuum state, because the wavelength of signal beam and local oscillator is different from each other and they can't interfere with each one. Recalling that the shot noise amplitude of the two-port UBHD output is  $\Delta X_T$  or  $\Delta P_T$  as shown in Eq. (12), scaling with  $\sqrt{2}|\alpha_{LO}|$  (cf. Eq. (7), generally, for heterodyne detection LO is split into two beams so its intensity should be divided by two), the measurements of Bob's detection are

$$\begin{aligned} \hat{x}_B &= \frac{\Delta i}{\sqrt{2}q|\alpha_{LO}|} = \frac{(1-2T_1)I_S^r - (1-2T_2)I_{LO}^r + 2\sqrt{I_S^r}\Delta X_S + 2\sqrt{I_{LO}^r}\Delta X_{LO}}{\sqrt{2}|\alpha_{LO}|} \\ &= \sqrt{\frac{\eta}{2}}\hat{x}_E + \frac{(1-2T_1)(-2\sqrt{T_1(1-T_1)}I_S X_N) - (1-2T_2)(-2\sqrt{T_2(1-T_2)}I_{LO} X_N) + 2\sqrt{I_S^r}\Delta X_S + 2\sqrt{I_{LO}^r}\Delta X_{LO}}{\sqrt{2}|\alpha_{LO}|} \\ &= \sqrt{\frac{\eta}{2}}\hat{x}_E + \hat{x}_{B|E}, \\ \hat{p}_B &= \frac{\Delta i}{\sqrt{2}q|\alpha_{LO}|} = \frac{(1-2T_1)I_S^t - (1-2T_2)I_{LO}^t + 2\sqrt{I_S^t}\Delta P_S + 2\sqrt{I_{LO}^t}\Delta P_{LO}}{\sqrt{2}|\alpha_{LO}|} \\ &= \sqrt{\frac{\eta}{2}}\hat{p}_E + \frac{(1-2T_1)(2\sqrt{T_1(1-T_1)}I_S X_N) - (1-2T_2)(2\sqrt{T_2(1-T_2)}I_{LO} X_N) + 2\sqrt{I_S^t}\Delta P_S + 2\sqrt{I_{LO}^t}\Delta P_{LO}}{\sqrt{2}|\alpha_{LO}|} \\ &= \sqrt{\frac{\eta}{2}}\hat{p}_E + \hat{p}_{B|E}, \end{aligned} \quad (15)$$

where  $\Delta i$  is the subtraction of two port outputs of UBHD proportional to the intensity difference of two beams and the proportional constant is  $q$ .  $\hat{x}_{B|E}$  or  $\hat{p}_{B|E}$  is the deviation of  $\hat{x}_B$  or  $\hat{p}_B$  from  $\hat{x}_E$  or  $\hat{p}_E$ . The conditional variance of Bob's measurements conditioned on Eve's can be computed as

tion of  $\hat{x}_B$  or  $\hat{p}_B$  from  $\hat{x}_E$  or  $\hat{p}_E$ . The conditional variance of Bob's measurements conditioned on Eve's can be computed as

$$\begin{aligned}
V_{B|E}^x &= \langle \hat{x}_{B|E}^2 \rangle = \frac{[(1-2T_1)(-2\sqrt{T_1(1-T_1)}I_S X_N)]^2}{2|\alpha_{LO}|^2} \\
&+ \frac{[(1-2T_2)(-2\sqrt{T_2(1-T_2)}I_{LO} X_N)]^2 + 4I_S^r(\Delta X_S)^2 + 4I_{LO}^r(\Delta X_{LO})^2}{2|\alpha_{LO}|^2} \\
&\approx \frac{2T_2(1-T_2)(1-2T_2)^2 I_{LO} N_0 + 2(1-T_2)I_{LO}[4T_2(1-T_2)N_0]}{|\alpha_{LO}|^2} \\
&\approx 2T_2(1-T_2)(1-2T_2)^2 N_0 + 8T_2(1-T_2)^2 N_0, \\
V_{B|E}^p &\approx V_{B|E}^x \equiv V_{B|E}.
\end{aligned} \tag{16}$$

The third line holds because  $I_S, I_S^r \ll |\alpha_{LO}|^2$ , and the forth line can be reduced for providing that the intensity of fake local oscillator ( $I_{LO} = |\alpha'_{LO}|^2$ ) Eve sends is the same as the original local oscillator ( $|\alpha_{LO}|^2$ ). Under this assumption,  $V_{B|E}^p$  is equivalent with  $V_{B|E}^x$  and both of them can be denoted as  $V_{B|E}$  for short.

In order to obtain the conditional variance ( $V_{B|A}$ ) of Bob's measurements conditioned on Alice's random optional Gaussian variables  $x_A$  or  $p_A$ , we can substitute Eq. (1) and (2) to Eq. (15) to achieve Bob's measurements about Alice's mode. That's

$$\begin{aligned}
\hat{x}_B &= \sqrt{\frac{\eta}{2}}(x_A + \hat{x}_N^A + \hat{x}_N^E) + \hat{x}_{B|E}, \\
\hat{p}_B &= \sqrt{\frac{\eta}{2}}(p_A + \hat{p}_N^A + \hat{p}_N^E) + \hat{p}_{B|E}.
\end{aligned} \tag{17}$$

Then, we can get the conditional variance  $V_{B|A}$

$$V_{B|A} = \langle (\hat{x}_B - \sqrt{\eta/2}x_A)^2 \rangle = \eta N_0 + V_{B|E}. \tag{18}$$

Interestingly, it's clear that  $V_{B|E}$  is always smaller than  $V_{B|A}$ , so the information between Bob and Eve is always much larger than that between Bob and Alice, which is consistent with the strategy Eve implements intercept-and-resend attack combined with wavelength attack that Eve totally knows Bob's measurements except some small deviation  $V_{B|E}$ . We will analyze this deviation accurately and investigate how Eve hides herself with this attack in next section.

### III. DISCUSSION AND CONCLUSION

As previous sections analyzed, if Eve implements this wavelength attack against Bob's practical system, the conditional variance  $V_{B|E}$  in Eq. (16) versus the transmittance  $T_2$  (comparing to the local oscillator) of ABS on Bob's side is plotted in Fig. 3.

When  $T_2$  equals 0.15 or 0.5,  $V_{B|E}$  will be  $N_0$  and can reach the maximum value  $1.24N_0$  when  $T_2$  equals 0.3. In practical heterodyne protocol of CVQKD, the secure conditional variance  $V_{B|A}$  is always  $N_0$  except for some small excess noise  $\varepsilon N_0$ . Consequently, Eve must select

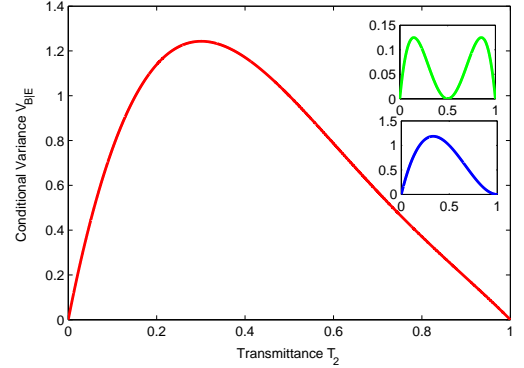


FIG. 3. (Color online) Conditional variance  $V_{B|E}$  vs. the transmittance  $T_2$  of ABS on Bob's side. Inset are the first term (upside) and the second term (downside) of Eq. (16)

appropriate  $T_2$  making  $V_{B|E}$  equal  $(1-\eta)N_0$ , then she can hide herself completely and get all information between Alice and Bob. Moreover, as Sec. II analyzed, different values of  $T_2$  can always make Eq. (3) satisfied namely Eve could implement this wavelength attack successfully in any case. Besides, from Eq. (16), it can be concluded that the main contribution to conditional variance  $V_{B|E}$  is the shot noise of two beams (especially local oscillator  $|\alpha'_{LO}|^2, |\alpha'_S|^2 \ll |\alpha_{LO}|^2$ , so the shot noise contributed by weak signal  $\alpha'_S$  can be neglected) transmitting through the two-port UBHD, and the noise introduced by the first ABS of Bob's side (as one-port UBHD) (Fig. 3 upside inset) can be neglected because of the large denominator  $|\alpha_{LO}|^2$  proportional to  $10^8 N_0$  [3]. Additionally, if Eve could reduce the intensity of two sending beams which are both smaller than the original local oscillator  $|\alpha_{LO}|^2$ , the conditional variance  $V_{B|E}$  can be decreased to any extent because the shot noise after being enlarged by the intensity of beam  $\alpha'_S$  or  $\alpha'_{LO}$  becomes small. And Eve can explore the wavelength-dependent property of additional monitoring ABS (splitting rate may be 1:99) to make the monitor recording intensity of the beam  $\alpha'_S$  or  $\alpha'_{LO}$  keep unchanged.

In conclusion, we investigate the feasibility of wavelength attack combined with intercept-resend method on practical CVQKD system with heterodyne protocol and

conclude that this attack will be implemented successfully if we choose appropriate transmittance  $T_2$  corresponding to the appropriate wavelength of fake local oscillator. This attack can be implemented successfully due to several reasons. First, we analyzed the solution of equations that two sending beams by Eve satisfied and it can be clearly seen that the solutions satisfying all conditions exist. Second, the main contribution of deviation of Bob's measurements from Eve's is due to the fake local oscillator's enlarging shot noise and can be reduced by selecting appropriate transmittance  $T_2$  or decreasing the intensity of fake local oscillator. These two aspects are unconsidered in Han's paper, which may leads their scheme invalid in some parameter regime. Last but not least, the transmittance of practical beam splitters at Bob's station is wavelength-dependent. However, if Bob

inserts optical filters on his system before receiving the light, this attack cannot be avoided efficiently as analyzed in Sec. II A, which is considered to be impossible in Han's paper. So using high quality filters and wavelength independent beam splitters in practical CVQKD systems and carefully monitoring local oscillator are very important to confirm the security of the heterodyne protocol of CVQKD.

## ACKNOWLEDGMENTS

This work is supported by the National Natural Science Foundation of China, Grant No. 61072071. L-M. L. is supported by the Program for New Century Excellent Talents.

- 
- [1] T. C. Ralph, Phys. Rev. A **61**, 010303(R) (1999).
  - [2] F. Grosshans, G. V. Asschee, J. Wenger, R. Brouri, N. Cerf, and P. Grangier, Nature (London) **421**, 238 (2003).
  - [3] J. Lodewyck *et al.*, Phys. Rev. A **76**, 042305 (2007).
  - [4] A. Leverrier and P. Grangier, Phys. Rev. Lett. **102**, 180504 (2009).
  - [5] Y. Shen, H-X. Zou, L. Tian, P-X Chen, and J-M Yuan, Phys. Rev. A **82**, 022317 (2010).
  - [6] P. Jouguet, S. Kunz-Jacques, and A. Leverrier, Phys. Rev. A **84**, 062317 (2011).
  - [7] C. Weedbrook, S. Pirandola, R. García-Patrón, N. J. Cerf, T. C. Ralph, J. H. Shapiro, and S. Lloyd, Rev. Mod. Phys. **84**, 621 (2012).
  - [8] V. Makarov, A. Anisimov, and J. Skaar, Phys. Rev. A **74**, 022313 (2006).
  - [9] Y. Zhao, C-H. F. Fung, B. Qi, C. Chen, and H. K. Lo, Phys. Rev. A **78**, 042333 (2008).
  - [10] S-H. Sun, M-S. Jiang, and L-M. Liang, Phys. Rev. A **83**, 062331 (2011).
  - [11] W-T. Liu, S-H. Sun, L-M. Liang, and J-M. Yuan, Phys. Rev. A **83**, 042326 (2011).
  - [12] S-H. Sun, M. Gao, M-S. Jiang, C-Y. Li, and L-M. Liang, Phys. Rev. A **85**, 032304 (2012).
  - [13] J. Lodewyck, T. Debuisschert, R. García-Patrón, R. Tualle-Brouri, N. J. Cerf, and P. Grangier, Phys. Rev. Lett. **98**, 030503 (2007).
  - [14] S-H. Sun, M-S. Jiang, and L-M. Liang, Phys. Rev. A **86**, 012305 (2012).
  - [15] H-W. Li, *et al.*, Phys. Rev. A **84**, 062308 (2011).
  - [16] J-Z. Huang, Z-Q. Yin, S. Wang, H-W. Li, W. Chen, G-C. Guo, and Z-F. Han, e-print arXiv:1206.6550v1 (2012).
  - [17] A. Ankiewicz, A. W. Snyder, and X. Zheng, J. Lightwave Technol. **4**, 1317 (1986).
  - [18] V. J. Tekippe, Fiber Integr. Opt. **9**, 97 (1990).
  - [19] H. P. Yuen and V. W. S. Chan, Opt. Lett. **8**, 177 (1983).
  - [20] B. L. Schumaker, Opt. Lett. **9**, 189 (1984).
  - [21] M. G. Raymer, J. Cooper, H. J. Carmichael, M. Beck, and D. T. Smithey, J. Opt. Soc. Am. B **12**, 1801 (1995).